ELSEVIER

Available online at www.sciencedirect.com

ScienceDirect

Journal of Number Theory 128 (2008) 2450–2458

JOURNAL OF Number Theory

www.elsevier.com/locate/jnt

A new family of imaginary quadratic fields whose class number is divisible by five

Yasuhiro Kishi

Department of Mathematics, Fukuoka University of Education, 1-1 Bunkyoumachi Akama, Munakata-shi, Fukuoka 811-4192, Japan

Received 17 August 2007; revised 18 January 2008

Available online 9 May 2008

Communicated by David Goss

Abstract

In this paper, we prove that the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-F_{50s+25}})$ $(s \geqslant 0)$ is divisible by 5, where F_n is the nth number in the Fibonacci sequence. Moreover we give a polynomial with integer coefficients whose splitting field over $\mathbb{Q}$ is an unramified cyclic quintic extension of $\mathbb{Q}(\sqrt{-F_{50s+25}})$.

1. Introduction

The following is a fundamental problem in the theory of quadratic fields: For a given positive integer N, find quadratic fields whose class number is divisible by N. Several authors (for example, T. Nagell [7], N.C. Ankeny and S. Chowla [1], Y. Yamamoto [12], P.J. Weinberger [11] and H. Ichimura [4]) gave an infinite family of quadratic fields whose class number is divisible by arbitrary given integer N. If limited to the case $N = 5$, C.J. Parry [8], J.-F. Mestre [6], M. Sase [10] and D. Byeon [2] gave a family of quadratic fields whose class number is divisible by 5. In particular, Sase [10] gave a family of polynomials whose splitting field is a D_5-extension of $\mathbb{Q}$ and an unramified C_5-extension of containing the quadratic field. In the present paper, we will give

E-mail address: ykishi@fukuoka-edu.ac.jp.

doi:10.1016/j.jnt.2008.02.016

other such polynomials by the use of a result of our previous paper [5]. As a consequence, we get the following new infinite family of quadratic fields whose class number is divisible by 5.

Theorem. *Let F_n denote the nth number in the Fibonacci sequence*:

$$1, 1, 2, 3, 5, 8, 13, \ldots.$$

Then the class number of the quadratic field $\mathbb{Q}(\sqrt{-F_{50s+25}})$ $(s \geqslant 0)$ *is divisible by* 5.

We list here those symbols which will be used throughout this article.

Let $\mathbb{Q}$ denote the field of rational numbers and $\mathbb{Z}$ denote the ring of rational integers.

For an integer n, let C_n and D_n denote the cyclic group of order n and the dihedral group of order $2n$, respectively.

For an extension L/K, denote the norm map and the trace map of L/K by $N_{L/K}$ and by $\mathrm{Tr}_{L/K}$, respectively. For simplicity, we denote N_L and Tr_L if the base field $K = \mathbb{Q}$. For a Galois extension L/K, we denote the Galois group of L/K by $\mathrm{Gal}(L/K)$.

For a polynomial $f(X)$ and a field K, we denote the minimal splitting field of $f(X)$ over K by $\mathrm{Spl}_K(f)$.

2. Statement of the results

To state our theorems, we prepare some notations.

Let (F_n) and (L_n) be the Fibonacci and the Lucas sequences, respectively, defined as follows:

$$F_1 = 1, \qquad F_2 = 1, \qquad F_{n+2} = F_{n+1} + F_n \quad (n \geqslant 1),$$
$$L_1 = 1, \qquad L_2 = 3, \qquad L_{n+2} = L_{n+1} + L_n \quad (n \geqslant 1).$$

Let $\zeta := e^{2\pi i/5}$ be a primitive fifth root of unity. For a non-negative integer m, we set $k_m := \mathbb{Q}(\sqrt{-F_{2m+1}})$. Moreover we define a cyclic quartic field M_m as follows: M_m is the proper subextension of $k_m(\zeta)/\mathbb{Q}(\sqrt{5})$ other than $k_m(\sqrt{5})$ and $\mathbb{Q}(\zeta)$. Then we can express $M_m = \mathbb{Q}(\sqrt{-F_{2m+1}}(\zeta - \zeta^{-1}))$. We define an element δ_m of M_m by

$$\delta_m := 1 + \varepsilon^m \sqrt{-F_{2m+1}}\bigl(\zeta - \zeta^{-1}\bigr),$$

where $\varepsilon := (1 + \sqrt{5})/2$ is a fundamental unit of $\mathbb{Q}(\sqrt{5})$. As we will see in Section 4, δ_m is a unit in M_m.

For a non-negative integer m, we define a polynomial $g_m(X)$ of degree 5 with integer coefficients by

$$g_m(X) := X^5 - 10X^3 - 20X^2 + 5\bigl(20F_{2m+1}^2 - 3\bigr)X + 40F_{2m+1}^2\bigl((-1)^m L_{2m+1} + 1\bigr) - 4.$$

Under the above notations and assumptions, we have the following.

Theorem 1. *Let m be a non-negative integer. Then the splitting field* $\mathrm{Spl}_{\mathbb{Q}}(g_m)$ *is a D_5-extension of $\mathbb{Q}$ containing k_m. If, moreover, $m \equiv 12 \pmod{5^2}$, then* $\mathrm{Spl}_{\mathbb{Q}}(g_m)$ *is an unramified cyclic quintic extension of k_m. Hence, by putting $m = 25s + 12$, the class number of the quadratic field* $\mathbb{Q}(\sqrt{-F_{50s+25}})$ *is divisible by* 5.

Theorem 2. *The set*

$$\{\mathbb{Q}(\sqrt{-F_{50s+25}}) \mid s \geqslant 0\}$$

is infinite.

3. D_5-polynomials

In this section, we give a parametric D_5-polynomial with integer coefficients. It is a review of [5] in the case $p = 5$ and the base field $\mathbb{Q}$.

Let ζ be a primitive fifth root of unity, and let $k = \mathbb{Q}(\sqrt{D})$ be a quadratic field which does not coincide with $\mathbb{Q}(\sqrt{5})$. Then there exists a unique proper subextension of the bicyclic biquadratic extension $k(\zeta)/\mathbb{Q}(\sqrt{5})$ other than $k(\sqrt{5})$ and $\mathbb{Q}(\zeta)$. We denote it by M. Then M is a cyclic quartic field. Let us call M *the associated field with* k. Fix the generator τ of $\mathrm{Gal}(k(\zeta)/k)$ with $\zeta^\tau = \zeta^2$, and define a subset $\mathcal{M}(k)$ of $k(\zeta)^\times$ as follows:

$$\mathcal{M}(k) := \{\gamma \in k(\zeta)^\times \mid \gamma^{3+4\tau+2\tau^2+\tau^3} \notin k(\zeta)^5\}.$$

For an element $\gamma \in M$, we define a polynomial $f_\gamma(X)$ by

$$\begin{aligned} f_\gamma(X) := X^5 &- 10N_M(\gamma)X^3 - 5N_M(\gamma)NT(\gamma)X^2 \\ &+ 5N_M(\gamma)\{N_M(\gamma) - NT(\gamma^{1+\tau})\}X - N_M(\gamma)NT(\gamma^{2+\tau}), \end{aligned}$$

where $NT = N_{\mathbb{Q}(\sqrt{5})}\mathrm{Tr}_{M/\mathbb{Q}(\sqrt{5})}$.

Applying [5, Theorem 2.1, Corollary 2.6] to the case $p = 5$, we get the following proposition.

Proposition 3.1. *Let the notation be as above. Then for $\delta \in \mathcal{M}(k) \cap M$, $\mathrm{Spl}_{\mathbb{Q}}(f_\delta)$ is a D_5-extension of $\mathbb{Q}$ containing k. Putting $E := \mathrm{Spl}_{\mathbb{Q}}(f_\delta)$, moreover, we have*

$$E = k\left(\mathrm{Tr}_{E(\zeta)/E}\left(\sqrt[5]{\delta^{3+4\tau+2\tau^2+\tau^3}}\right)\right).$$

Remark 3.2. In [5], we can see that *every* D_5-extension E of $\mathbb{Q}$ containing k is given as $E = \mathrm{Spl}_{\mathbb{Q}}(f_\delta)$ for some $\delta \in \mathcal{M}(k) \cap M$.

4. Properties of Fibonacci and Lucas numbers

There are many relations between Fibonacci and Lucas numbers. (See, for example [9].) In this section, we list six properties which we need in the proof of our theorems.

(A) The power of $\varepsilon = (1 + \sqrt{5})/2$ is expressed by

$$\varepsilon^m = \frac{L_m + F_m\sqrt{5}}{2}.$$

(B) For positive integer m, we have

$$F_{m+1} = \frac{L_m + F_m}{2}.$$

(C) For any positive integer N, the Fibonacci and the Lucas sequence have a period modulo N, that is, there exists $l, l' \in \mathbb{Z}$ such that

$$F_{a+bl} \equiv F_a \pmod{N}, \qquad L_{a+bl'} \equiv L_a \pmod{N}$$

for any positive integers a, b. (We call l and l' *the length of period modulo* N.)

(D) For positive integer m,

$$\begin{aligned} 5^2 \mid F_m &\iff 5^2 \mid m, \\ 5^3 \mid F_m &\iff 5^3 \mid m. \end{aligned}$$

(E) F_n is a perfect square if and only if $n = 1, 2, 12$.

(F) Let n and m be positive integers. If $d = \gcd(n, m)$, then we have

$$\gcd(F_n, F_m) = F_d.$$

Remark 4.1. Property (E) is proved by J.H.E. Cohn [3]. The others are easily proved.

5. Proof of Theorem 1

Let the notation be as in Section 2. Then M_m is the associated field with k_m. Hence we can apply Proposition 3.1. Let τ be a generator of $\mathrm{Gal}(k_m(\zeta)/k_m)$ ($\cong C_4$) with $\zeta^\tau = \zeta^2$. Now let us calculate $f_{\delta_m}(X)$;

$$\begin{aligned} f_{\delta_m}(X) = {}& X^5 - 10N_{M_m}(\delta_m)X^3 - 5N_{M_m}(\delta_m)NT(\delta_m)X^2 \\ &+ 5N_{M_m}(\delta_m)\bigl\{N_{M_m}(\delta_m) - NT\bigl(\delta_m^{1+\tau}\bigr)\bigr\}X - N_{M_m}(\delta_m)NT\bigl(\delta_m^{2+\tau}\bigr). \end{aligned}$$

We note that τ satisfies the following:

$$\zeta^\tau = \zeta^2, \qquad (\sqrt{5})^\tau = -\sqrt{5}, \qquad (\sqrt{-F_{2m+1}})^\tau = \sqrt{-F_{2m+1}}.$$

Write $\bar{\varepsilon} := \varepsilon^\tau$; then we have

$$\begin{aligned} N_{M_m}(\delta_m) &= \bigl(1 + \varepsilon^m\sqrt{-F_{2m+1}}\bigl(\zeta - \zeta^{-1}\bigr)\bigr)\bigl(1 + \bar{\varepsilon}^m\sqrt{-F_{2m+1}}\bigl(\zeta^2 - \zeta^{-2}\bigr)\bigr) \\ &\quad \times \bigl(1 - \varepsilon^m\sqrt{-F_{2m+1}}\bigl(\zeta - \zeta^{-1}\bigr)\bigr)\bigl(1 - \bar{\varepsilon}^m\sqrt{-F_{2m+1}}\bigl(\zeta^2 - \zeta^{-2}\bigr)\bigr) \\ &= \bigl(1 + \varepsilon^{2m}F_{2m+1}\bigl(\zeta - \zeta^{-1}\bigr)^2\bigr)\bigl(1 + \bar{\varepsilon}^{2m}F_{2m+1}\bigl(\zeta^2 - \zeta^{-2}\bigr)^2\bigr) \\ &= \left(1 - \frac{5+\sqrt{5}}{2}\varepsilon^{2m}F_{2m+1}\right)\left(1 - \frac{5-\sqrt{5}}{2}\bar{\varepsilon}^{2m}F_{2m+1}\right) \end{aligned}$$

$$
\begin{aligned}
&= 1 - \frac{5+\sqrt{5}}{2}\varepsilon^{2m} F_{2m+1} - \frac{5-\sqrt{5}}{2}\bar{\varepsilon}^{2m} F_{2m+1} + 5N_{\mathbb{Q}(\sqrt{5})}(\varepsilon)^{2m} F_{2m+1}^2 \\
&= 1 - F_{2m+1}\left\{\mathrm{Tr}_{\mathbb{Q}(\sqrt{5})}\left(\frac{5+\sqrt{5}}{2}\varepsilon^{2m}\right) - 5F_{2m+1}\right\},
\end{aligned}
$$

by using

$$
\left(\zeta - \zeta^{-1}\right)^2 = \left(2i \sin\frac{2\pi}{5}\right)^2 = -\frac{5+\sqrt{5}}{2}, \qquad \left(\zeta^2 - \zeta^{-2}\right)^2 = \left(2i \sin\frac{4\pi}{5}\right)^2 = -\frac{5-\sqrt{5}}{2}.
$$

Here, by Property (B) we have

$$
\begin{aligned}
\mathrm{Tr}_{\mathbb{Q}(\sqrt{5})}\left(\frac{5+\sqrt{5}}{2}\varepsilon^{2m}\right) &= \mathrm{Tr}_{\mathbb{Q}(\sqrt{5})}\left(\frac{5+\sqrt{5}}{2}\cdot\frac{L_{2m}+F_{2m}\sqrt{5}}{2}\right) \\
&= \frac{5L_{2m}+5F_{2m}}{2} \\
&= 5F_{2m+1}.
\end{aligned}
$$

Therefore we get $N_{M_m}(\delta_m) = 1$. By similar calculations, we have

$$
\begin{aligned}
NT(\delta_m) &= 4, \\
NT\left(\delta_m^{1+\tau}\right) &= 4 - 20F_{2m+1}^2, \\
NT\left(\delta_m^{2+\tau}\right) &= 4 - 40F_{2m+1}^2\left(1 + (-1)^m L_{2m+1}\right).
\end{aligned}
$$

Substituting them into $f_{\delta_m}(X)$, we have

$$
\begin{aligned}
f_{\delta_m}(X) &= X^5 - 10X^3 - 20X^2 + 5\left(20F_{2m+1}^2 - 3\right)X + 40F_{2m+1}^2\left((-1)^m L_{2m+1} + 1\right) - 4 \\
&= g_m(X).
\end{aligned}
$$

Now we consider when the assumption $\delta_m \in \mathcal{M}(k_m)$ of Proposition 3.1 holds, that is, $\delta_m^{3+4\tau+2\tau^2+\tau^3}$ is not a fifth power in $k_m(\zeta)$.

Suppose that $\delta_m^{3+4\tau+2\tau^2+\tau^3}$ is a fifth power in $k_m(\zeta)$; $\delta_m^{3+4\tau+2\tau^2+\tau^3} = \alpha^5$, $\alpha \in k_m(\zeta)$. Since $k_m(\zeta)$ is normal over $\mathbb{Q}$, we have

$$
\mathrm{Tr}_{E(\zeta)/E}\left(\sqrt[5]{\delta_m^{3+4\tau+2\tau^2+\tau^3}}\right) = \mathrm{Tr}_{E(\zeta)/E}(\alpha) \in k_m(\zeta),
$$

where $E = \mathrm{Spl}_{\mathbb{Q}}(g_m)$. By the last half of Proposition 3.1, therefore, we have

$$
\mathrm{Spl}_{\mathbb{Q}}(g_m) = k_m\left(\mathrm{Tr}_{E(\zeta)/E}(\alpha)\right) \subset k_m(\zeta).
$$

Hence the degree $[\mathrm{Spl}_{\mathbb{Q}}(g_m) : k_m]$ is less than 5. Then $g_m(X)$ must be reducible over $\mathbb{Q}$. Conversely, suppose that $\delta_m \in \mathcal{M}(k_m)$. Then by Proposition 3.1, we have $[\mathrm{Spl}_{\mathbb{Q}}(g_m) : k_m] = 5$, and so $g_m(X)$ is irreducible over $\mathbb{Q}$. Therefore, we have

Proposition 5.1. *It hold that $\delta_m \in \mathcal{M}(k_m)$ if and only if $g_m(X)$ is irreducible over $\mathbb{Q}$.*

From now on, we assume that $m \equiv 12 \pmod{5^2}$. First we will show that $\delta_m \in \mathcal{M}(k_m)$. Note that together the Fibonacci and the Lucas sequences have a period of the same length 50 modulo the prime 151 (cf. Property (C)). By putting $m = 25s + 12$, we have

$$F_{2m+1} = F_{50s+25} \equiv 129 \pmod{151} \quad \text{and} \quad L_{2m+1} = L_{50s+25} \equiv 0 \pmod{151}.$$

Then we have

$$g_m(X) \equiv X^5 - 10X^3 - 20X^2 + 65X + 28 \pmod{151}.$$

We see that the right-hand side is irreducible modulo 151. Then $g_m(X)$ is irreducible over $\mathbb{Q}$. From Proposition 5.1, we get $\delta_m \in \mathcal{M}(k_m)$.

By Proposition 3.1, $\mathrm{Spl}_{\mathbb{Q}}(g_m)$ $(= \mathrm{Spl}_{\mathbb{Q}}(f_{\delta_m}))$ is a D_5-extension of $\mathbb{Q}$ containing k_m. We will finally show that the cyclic quintic extension $\mathrm{Spl}_{\mathbb{Q}}(g_m)/k_m$ is unramified. Let θ be a root of $g_m(X)$. Let q be a prime number in general. A prime divisor of q in k_m is ramified in $\mathrm{Spl}_{\mathbb{Q}}(g_m)$ if and only if q is totally ramified in $\mathbb{Q}(\theta)$ because $[\mathrm{Spl}_{\mathbb{Q}}(g_m) : k_m]$ and $[k_m : \mathbb{Q}]$ are relatively prime. Hence we have only to verify that no primes are totally ramified in $\mathbb{Q}(\theta)$. This can be proved by using the following Sase's result. For a prime number p and for an integer m, we denote the greatest exponent μ of p such that $p^\mu \mid m$ by $v_p(m)$.

Proposition 5.2. *(See [10, Proposition 2].) Let p $(\neq 2)$ and q be prime numbers. Suppose that the polynomial*

$$\varphi(X) = X^p + \sum_{j=0}^{p-2} a_j X^j, \quad a_j \in \mathbb{Z},$$

is irreducible over $\mathbb{Q}$ and satisfies the condition

$$v_q(a_j) < p - j \quad \text{for some } j,\ 0 \leqslant j \leqslant p-2. \tag{5.1}$$

Let θ be a root of $\varphi(X)$.

(1) *If q is different from p, then q is totally ramified in $\mathbb{Q}(\theta)/\mathbb{Q}$ if and only if*

$$0 < \frac{v_q(a_0)}{p} \leqslant \frac{v_q(a_j)}{p-j} \quad \text{for every } j,\ 1 \leqslant j \leqslant p-2.$$

(2) *The prime p is totally ramified in $\mathbb{Q}(\theta)/\mathbb{Q}$ if and only if one of the following conditions* (S-i), (S-ii) *holds*:

$$\text{(S-i)} \quad 0 < \frac{v_p(a_0)}{p} \leqslant \frac{v_p(a_j)}{p-j} \quad \text{for every } j,\ 1 \leqslant j \leqslant p-2;$$

$$\text{(S-ii)} \quad \text{(S-ii-1)} \quad v_p(a_0) = 0,$$

$$\text{(S-ii-2)} \quad v_p(a_j) > 0 \quad \text{for every } j,\ 1 \leqslant j \leqslant p-2,$$

$$\text{(S-ii-3)}\quad \frac{v_p(\varphi(-a_0))}{p} \leqslant \frac{v_p(\varphi^{(j)}(-a_0))}{p-j} \quad \textit{for every } j,\ 1 \leqslant j \leqslant p-2, \quad \textit{and}$$

$$\text{(S-ii-4)}\quad v_p\big(\varphi^{(j)}(-a_0)\big) < p-j \quad \textit{for some } j,\ 0 \leqslant j \leqslant p-1,$$

where $\varphi^{(j)}(X)$ *is the* j*th differential of* $\varphi(X)$.

Now let us apply Proposition 5.2 to our polynomial $g_m(X)$. First, we easily verify that $g_m(X)$ satisfies (5.1) for each prime. Next, we see from (1) of Proposition 5.2 that no primes except for 5 are totally ramified in $\mathbb{Q}(\theta)/\mathbb{Q}$ because the greatest common divisor of the coefficient of X^3 and that of X is equal to 5. We will show, therefore, that 5 is not totally ramified. Denote the constant term of $g_m(X)$ by c_0;

$$c_0 := 40F_{2m+1}^2\big((-1)^m L_{2m+1} + 1\big) - 4.$$

Since c_0 is not divisible by 5, the condition (S-i) does not hold. By the assumption $m \equiv 12 \pmod{5^2}$, we have $2m+1 \equiv 0 \pmod{5^2}$. Then by Property (D), we have $F_{2m+1} \equiv 0 \pmod{5^2}$, and hence $-c_0 \equiv 4 \pmod{5^5}$. Therefore we have

$$\begin{aligned}
g_m(-c_0) &\equiv 4^5 - 10\cdot 4^3 - 20\cdot 4^2 - 15\cdot 4 - 4 \equiv 0 \pmod{5^5},\\
g_m^{(1)}(-c_0) &\equiv 5\cdot 4^4 - 30\cdot 4^2 - 40\cdot 4 - 15 \equiv 0 \pmod{5^4},\\
g_m^{(2)}(-c_0) &\equiv 20\cdot 4^3 - 60\cdot 4 - 40 \equiv 0 \pmod{5^3},\\
g_m^{(3)}(-c_0) &\equiv 60\cdot 4^2 - 60 \equiv 0 \pmod{5^2}.
\end{aligned}$$

Then the condition (S-ii-4) does not hold. (We can easily check that (S-ii-1), (S-ii-2) and (S-ii-3) hold.) Hence 5 is not totally ramified in $\mathbb{Q}(\theta)$. This completes the proof of Theorem 1.

6. Proof of Theorem 2

Assume, for a contradiction, $\#\{\mathbb{Q}(\sqrt{-F_{50s+25}}) \mid s \geqslant 0\} < \infty$. For an integer m, we denote the square free part of m by $\mathrm{sf}(m)$. By the assumption, the set

$$\mathcal{P} := \bigcup_{s\geqslant 0}\big\{\text{prime factors of } \mathrm{sf}(F_{50s+25})\big\}$$

is finite. Then there exists a positive integer t so that we have

$$\mathcal{P} = \bigcup_{0\leqslant s\leqslant t}\big\{\text{prime factors of } \mathrm{sf}(F_{25(2s+1)})\big\}.$$

Take a prime q with $q > 2t+1$ and $q \neq 5$. Then for each prime factor r of $\mathrm{sf}(F_{25q})$, we have

$$\mathrm{sf}(F_{25(2s+1)}) \equiv 0 \pmod r \quad \text{for some } s,\ 0 \leqslant s \leqslant t. \tag{6.1}$$

(Note that $\mathrm{sf}(F_{25q}) > 1$ by Property (E).) On the other hand, because q is prime, for each s, $0 \leqslant s \leqslant t$, we have

$$\gcd\bigl(25(2s+1), 25q\bigr) = 25,$$

and hence by Property (F),

$$\gcd(F_{25(2s+1)}, F_{25q}) = F_{25} = 3001 \cdot 5^2.$$

Then we have $r = 5$ or 3001. Moreover, by Property (D), we have $5^2 \parallel F_{25q}$ and hence $r = 3001$. Then we can express

$$F_{25q} = 3001 A_q^2$$

for some $A_q \in \mathbb{Z}$. Then we have

$$-1 = N_{\mathbb{Q}(\sqrt{5})}\bigl(\varepsilon^{25q}\bigr) = \frac{L_{25q}^2 - 5F_{25q}^2}{4} = \frac{L_{25q}^2 - 5 \cdot 3001^2 A_q^4}{4}.$$

This implies that (A_q, L_{25q}) is an integer solution of the equation

$$Y^2 = 5 \cdot 3001^2 X^4 - 4. \tag{6.2}$$

The values of L_{25q} (q is prime), of course, are different from each other. However by Siegel's theorem, there are only finitely many integer solutions (X, Y) of Eq. (6.2). This is a contradiction. The proof of Theorem 2 is completed.

7. Numerical examples

Example 7.1. Let $m = 12$. By $F_{12} = 144$, $L_{12} = 322$ and $F_{25} = 3001 \cdot 5^2$, we have

$$\delta_{12} = 1 + \frac{322 + 144\sqrt{5}}{2}\sqrt{-3001 \cdot 5^2}\bigl(\zeta - \zeta^{-1}\bigr)$$

and

$$g_{12}(X)\bigl(= f_{\delta_{12}}(X)\bigr) = X^5 - 10X^3 - 20X^2 + 562875062485X + 37771618494049996.$$

By Theorem 1, the splitting field of $g_{12}(X)$ is an unramified cyclic quintic extension of $\mathbb{Q}(\sqrt{-F_{25}}) = \mathbb{Q}(\sqrt{-3001})$.

In Table 1, we list the prime decompositions of $-F_{50s+25}$ and the structure of the ideal class groups of $\mathbb{Q}(\sqrt{-F_{50s+25}})$ for $0 \leqslant s \leqslant 3$. For this table we use GP/PARI (Version 2.1.5).

Table 1

s	$-F_{50s+25}$	Structure of the ideal class group of $\mathbb{Q}(\sqrt{-F_{50s+25}})$
0	$-3001 \cdot 5^2$	C_{40}
1	$-2 \cdot 61 \cdot 3001 \cdot 230686501 \cdot 5^2$	$C_{2461460} \times C_2 \times C_2$
2	$-5 \cdot 3001 \cdot 158414167964045700001 \cdot 5^2$	$C_{79285156360} \times C_8 \times C_2$
3	$-13 \cdot 701 \cdot 3001 \cdot 141961 \cdot 17231203730201189308301 \cdot 5^2$	$C_{1737032019043290} \times C_6 \times C_2 \times C_2 \times C_2$

Acknowledgment

The author would like to thank the referee for his/her careful reading and comments that led to the improvement of this paper.

References

[1] N.C. Ankeny, S. Chowla, On the divisibility of the class number of quadratic fields, Pacific J. Math. 5 (1955) 321–324.
[2] D. Byeon, Real quadratic fields with class number divisible by 5 or 7, Manuscripta Math. 120 (2006) 211–215.
[3] J.H.E. Cohn, On square Fibonacci numbers, J. London Math. Soc. 39 (1964) 537–540.
[4] H. Ichimura, Note on the class numbers of certain real quadratic fields, Abh. Math. Sem. Univ. Hamburg 73 (2003) 281–288.
[5] M. Imaoka, Y. Kishi, On dihedral extensions and Frobenius extensions, in: Galois Theory and Modular Forms, in: Dev. Math., vol. 11, Kluwer Acad. Publ., Boston, MA, 2004, pp. 195–220.
[6] J.-F. Mestre, Courbes elliptiques et groupes de classes d'idéaux de certains corps quadratiques, J. Reine Angew. Math. 343 (1983) 23–35.
[7] T. Nagell, Über die Klassenzahl imaginär-quadratischer Zahlköper, Abh. Math. Sem. Univ. Hamburg 1 (1922) 140–150.
[8] C.J. Parry, On the class number of relative quadratic fields, Math. Comp. 32 (1978) 1261–1270.
[9] P. Ribenboim, The New Book of Prime Number Records, Springer-Verlag, New York, 1996.
[10] M. Sase, On a family of quadratic fields whose class numbers are divisible by five, Proc. Japan Acad. Ser. A Math. Sci. 74 (1998) 120–123.
[11] P.J. Weinberger, Real quadratic fields with class numbers divisible by n, J. Number Theory 5 (1973) 237–241.
[12] Y. Yamamoto, On unramified Galois extensions of quadratic number fields, Osaka J. Math. 7 (1970) 57–76.